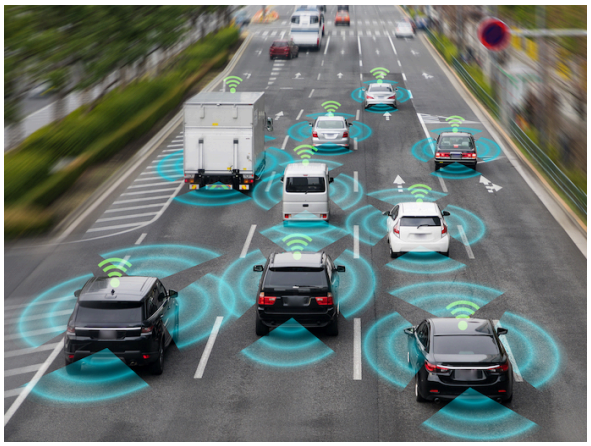
Artificial Intelligence based cybersecurity for connected and automated vehicles

Resultados resumidos

Vehículos inteligentes más ciberseguros

La seguridad y la protección de los vehículos «inteligentes» autónomos y conectados, que cada vez transportan más personas y carga, constituyen una preocupación al alza. El equipo del proyecto CARAMEL propone una tecnología integral de ciberseguridad para vehículos consciente de los riesgos y basada en procesos, desde el diseño hasta el funcionamiento.

SEGURIDAD



© Metamorworks/Shutterstock.com

Si bien los avances en conectividad e inteligencia artificial han favorecido muchas prestaciones inteligentes en los vehículos de carretera modernos, también han propiciado que se comentan delitos informáticos sofisticados que aprovechan las lagunas de seguridad.

En casos extremos, una ciberseguridad deficiente pone en peligro la protección de los pasajeros, los peatones, otros vehículos y las infraestructuras críticas. Lo más frecuente, sin embargo, es que se produzcan robos de vehículos o filtraciones de datos sensibles.

«Los vehículos son cada vez más “centros de datos sobre ruedas”, lo que los hace vulnerables a ataques. Para mejorar la aceptación de vehículos más seguros, inteligentes y ecológicos, hay que poder confiar en ellos, por lo que la ciberseguridad es fundamental», comenta Jordi Guijarro Olivares, coordinador del proyecto CARAMEL.

El equipo de este proyecto financiado con fondos europeos, coordinado por la

Fundación i2CAT, desarrolló estrategias de mitigación para las principales vulnerabilidades de seguridad en cuatro áreas operativas prioritarias.

«Nuestro sistema “Cooperative Situational Awareness” lleva la ciberseguridad mas allá de la simple lucha contra los ataques informáticos más avanzados al establecer un planteamiento más unificado de protección gracias al empleo de los sensores de los vehículos para desarrollar resiliencia», explica Peter Hofmann, coordinador técnico del proyecto CARAMEL.

Cuatro pilares de la ciberseguridad

El planteamiento de CARAMEL consistió en introducir tecnologías de ciberseguridad, tanto en los vehículos como en la infraestructura de respaldo, fundamentadas en cuatro pilares. Los tres primeros se probaron en las instalaciones de Panasonic a principios de este año.

El primer pilar, movilidad autónoma, introdujo técnicas de aprendizaje automático (AA) para detectar amenazas a la interfaz de radio y a los sensores a fin de proteger las funcionalidades de los vehículos autónomos, como el reconocimiento de escena, así como sus sensores a bordo (cámaras, radar óptico, GPS, etc.).

El equipo del proyecto también desarrolló un nuevo dispositivo de antipirateo informático, como parte de la unidad de control a bordo, capaz de enviar análisis de datos a bordo para su procesamiento o visualización posterior.

Para entrenar y validar el AA, se emplearon conjuntos de datos reales y de simulación procedentes de fuentes públicas y de los socios.

«La demostración final superó las expectativas y demostró su consistencia frente a una amplia variedad de ataques y niveles de gravedad. Nuestro dispositivo de antipirateo informático detectó satisfactoriamente ataques contra sensores, como la suplantación de ubicación GPS y las anomalías en señales de tráfico, lo que mejoró la conciencia situacional del espacio del vehículo», agrega Olivares.

El segundo pilar, movilidad conectada, se basó en la detección de ataques en vehículos conectados. El equipo ejecutó protocolos de comunicación vehículo a todo que permitieron la comunicación entre vehículos y con unidades de comunicación en la carretera.

Además, en CARAMEL se desarrolló una tecnología colaborativa, a través de la cual los vehículos trabajan juntos para identificar ataques de suplantación de ubicación GPS, activando capacidades de privacidad avanzadas en respuesta.

El trabajo en el segundo pilar dio lugar asimismo a una arquitectura que conectaba las alarmas de los vehículos a servidores en la nube. Cuando se activan por un ataque, también activan protocolos de seguridad o supervisan la actividad.

En el tercer pilar, electromovilidad, se crearon motores de detección de inteligencia artificial en la nube para identificar a distancia ataques informáticos en estaciones de recarga. Esto se logra al detectar anomalías en la comunicación entre una estación y sus procesos de gestión remotos.

«Muchas estaciones de recarga tienen “hardware” o “software” obsoletos, por lo que no cumplen con las normas de seguridad más recientes. En este sentido, descubrimos que el uso de técnicas estadísticas como la correlación de Pearson y los bosques aleatorios reducían de forma significativa la complejidad de los modelos de AA necesarios para detectar anomalías y protegerlos», comenta Petros Kapsalas, responsable de pruebas del proyecto CARAMEL.

El cuarto pilar, vehículo teledirigido, está aún en desarrollo por parte de los socios surcoreanos del proyecto, a quienes les queda otro año de financiación.

El equipo surcoreano trabaja en el diseño de la arquitectura de procesamiento de datos y en la tecnología de detección de amenazas necesarias para que los vehículos teledirigidos 5G sean más seguros.

Ciberseguridad de última generación

Dado que el transporte forma parte de las infraestructuras críticas de Europa, está destinado a una protección especial en tiempos de crisis y se considera un pilar central de la Estrategia de Ciberseguridad de la Unión Europea.

Guijarro concluye: «Los resultados de CARAMEL constituyen un salto adelante hacia la ciberseguridad de última generación para vehículos autónomos, conectados y eléctricos. Pero para que los agentes europeos se puedan beneficiar de ella, primero habría que abordar la fragmentación de la industria y las políticas».

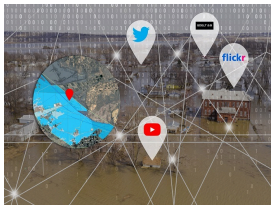
Palabras clave

CARAMEL, seguridad, inteligente, autónomo, conectado, ciberseguridad, inteligencia artificial, aprendizaje automático, delito informático, datos, 5G

Descubra otros artículos del mismo campo de aplicación

Un dron vigila en los rescates marítimos

Eliminar las credenciales estáticas para proteger los dispositivos del internet de las cosas



Las redes sociales, la colaboración masiva y la IA se unen para ubicar eventos en tiempo casi real

Refuerzo de la resiliencia de los hospitales frente a las amenazas

Información del proyecto

CARAMEL

Financiado con arreglo a

Identificador del acuerdo de subvención:
833611

Sitio web del proyecto

DOI
10.3030/833611

Proyecto cerrado

Fecha de la firma de la CE
27 Septiembre 2019

Fecha de inicio
1 Octubre 2019

Fecha de finalización
30 Junio 2022

INDUSTRIAL LEADERSHIP - Leadership in enabling and industrial technologies - Information and Communication Technologies (ICT)

Coste total
€ 7 033 655,10

Aportación de la UE
€ 4 998 503,51

Coordinado por
FUNDACIO PRIVADA I2CAT, INTERNET I INNOVACIO DIGITAL A CATALUNYA
Spain

Última actualización: 4 Noviembre 2022

Permalink: https://cordis.europa.eu/article/id/442445-making-smart-vehicles-more-cybersecure/es

European Union, 2025